This extract of the Information Security Policies serves to highlight the information security practices that Contractors' / Consultant's employees or agents have to comply with when they are working in Tuas Power's premises, or connected to Tuas Power's network.

1. Loan of Keys to Secure Areas to Others

Employees/Contractors/Consultants shall not loan keys, both physical and electronic, to any unauthorized personnel.
(*Refer Tuas Power Information Security Policies, TP ISPPM, 2.1.5*)

2. Downloading Files and Information from the Internet

There are significant information security risks when downloading information and files from the Internet. Care must be taken to safeguard against malicious code, unlicensed applications and also inappropriate material. Information on the Internet may be inaccurate, invalid, deliberately misleading or may have legal implications. User must understand the consequences before starting to download.
(*Refer TP ISPPM 3.1.1*)

3. Receiving Electronic Mail (E-mail)

Workstations or notebooks used to receive e-mail must be installed with antivirus applications and updated with the latest virus information data file. Incoming e-mails must be treated with care due to its inherent Information Security risks.
(*Refer TP ISPPM 3.1.5*)

4. Receiving Unsolicited E-mail

Unsolicited e-mails shall be treated with caution.
(*Refer TP ISPPM 3.1.6*)

5. Forwarding E-mail

Users must ensure that information they are forwarding by e-mail (especially with attachments) is sent only to the appropriate persons and correctly addressed.
(*Refer TP ISP M3.1.7*)

6. Transferring and Exchanging Data

Sensitive or confidential data/information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured, e.g. by using encryption techniques, zipped with password, etc.
(*Refer TP ISPPM 3.4.1*)

7. Deleting "Temp" Files

Temporary files on users' PCs and laptops are to be deleted regularly.
(*Refer TP ISPPM 3.4.10*)

8. Saving Data / Information by Individual Users

In the process of creating or amending data files, user must save their work on the system regularly to prevent corruption or loss through system or power interruption.
(*Refer TP ISPPM 3.4.11*)

9. Sending Information to Third Parties

Prior to sending information to third parties, the intended recipient must be authorized to receive such information, and if necessary to enter into a non-disclosure agreement.
(*Refer TP ISPPM 3.7.3)*

10. Printing of Classified Documents

Confidential information, if printed to a network printer, shall be retrieved immediately by the authorized person when the print job has been sent to the printer.
(*Refer TP ISPPM 3.7.8*)

11. Company's Ownership of Intellectual Property Rights

All employees and third party contractors/consultants are to acknowledge that the intellectual property rights of work undertaken during their terms of employment/contract respectively belong to the Company unless otherwise stated in the contract.
(*Refer TP ISPPM 4.2.4*)

12. Information stored in Company's Systems

The Company reserves the right to have access to all information created and stored in the Company's Systems.
(*Refer TP ISPPM 4.2.5*)

13. Reporting to Information Security Committee

Employees/Contractors/Consultants must report the following to IT:

a. Identified, suspected, or witness of information security incidents or breaches;
b. Identified or suspected information security weaknesses

(*Refer TP ISPPM 5.1.1*)

14. Recording Evidence of Information Security Incidents

All Employees/Contractors/Consultants shall be aware that evidence of information security incidents will be formally recorded, and retained by the Information Security Working Group.
(*Refer TP ISPPM 5.1.2)*

15. Clear Screen Policy

All users of workstations and notebooks shall ensure that equipment is switched off, or enabled with password protected screen saver. This is to prevent pre-meditated or opportunistic attempts to read and copy data from systems when the equipment is left unattended even for a short period.
(*Refer TP ISPPM 7.6.4*)

16. Loading Personal Screen Savers

Employees/Contractors/Consultants shall not load any personal screen savers onto the Computers as it exposes the risk of a virus or malware infection.
(*Refer TP ISPPM 8.6.4*)